

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

United States of America)
)
)
 No. 14 CR 390
v.)
)
Tyler Lang)
)

DEFENDANT TYLER LANG'S RESPONSE TO THE
GOVERNMENT'S APPLICATION FOR AN ORDER RELATING TO SUBJECT PHONE 3

The government submitted an application requesting that this Court order Verizon Wireless to provide records related to telephone number (310) 617-2280 (“Subject Phone 3”), currently used by Tyler Lang. (Dkt. #65) The application seeks information from the time period from May 1, 2013, through August 14, 2013, and falls into two categories: 1) historical cell site location information (“CSLI”), and 2) historical toll record information. Defendant **Tyler Lang**, by the Federal Defender Program and its attorney **Geoffrey M. Meyer**, objects to the application and in support states the following:

FACTUAL BASIS

On August 15, 2013, police in Woodford County, Illinois, subjected Tyler Lang and Kevin Johnson to a traffic stop. Both Mr. Lang and Mr. Johnson were arrested during the traffic stop and charged with various state crimes related to vandalism that occurred the previous day at a mink ranch in Morris, Illinois.

Mr. Lang and Mr. Johnson were detained beginning the day of their arrest. After their arrest, law enforcement officers seized from their vehicle, among other things, two cell phones (Subject Phones 1 and 2). On September 9, 2013, the government requested and received from Chief Judge Castillo orders to obtain subscriber information, toll records, and historic CSLI for Subject Phones 1 and 2. Verizon and Tracfone, the providers for the two phones, complied with the orders no later than September 20, 2013. Subsequently, the contents of Subject Phones 1 and 2 were searched by the FBI. The results of the searches were available to the FBI no later than October 31, 2013.

On November 6, 2013, Mr. Lang pleaded guilty to possessing burglary tools (a class 4 felony) in Illinois state court. He was sentenced to 30 months' conditional discharge and 170 days' jail. After accounting for time served and good time credit, Mr. Lang was released from jail on November 8, 2013. On July 8, 2014, both Mr. Lang and Mr. Johnson, who was still in custody, were charged with two counts of violating the Animal Enterprise Terrorism Act, 18 U.S.C. § 43. Currently pending before the Court is Defendants' motion to dismiss the indictment. (Dkt. 63)

ARGUMENT

I. The proper standards to apply to the government's application.

The Stored Communications Act ("SCA") provides for the issuance of a court order to require a provider of electronic communications service or a remote computing service to disclose records of these services upon the government's offering of "specific and articulable facts showing that there are reasonable grounds

to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(c), (d). The “reasonable grounds to believe” standard “is less stringent than probable cause” required to obtain a search warrant under the Fourth Amendment. *See In re Application of the United States for an Order Directing a Provider of Elec. Communications Serv. to Disclose Records to the Gov’t*, 620 F.3d 304, 315 (3d Cir. 2010) (hereinafter “*In re Application of the U.S.*”). In this case, the government seeks information that falls into two categories: 1) historical CSLI, and 2) historical toll record information. Each requires a separate analysis.

Mr. Lang does not dispute that the lower “reasonable grounds to believe” standard applies to historical toll record information. In *Smith v. Maryland*, 442 U.S. 735 (1979), the Supreme Court held that no Fourth Amendment interests are implicated when the telephone company, at police request, utilizes a pen register to preserve or create evidence that otherwise would not exist, and then turns that evidence over to the police. By analogy, no Fourth Amendment interests would be implicated if a telephone company complies with a court order for a subscriber’s toll records. Thus, the “reasonable grounds to believe” standard found in the SCA creates by statute greater protection for toll records than that found in the Constitution, and is the applicable standard to the toll records sought in this case.

The same cannot be said for the historical CSLI the government seeks. Although the SCA purports to apply the same “reasonable grounds to believe” standard to

historical cell site information, the Fourth Amendment's warrant requirement trumps the statute because individuals have a reasonable expectation of privacy against governmental intrusion and this expectation applies to emerging technologies, such as CSLI.

The SCA, in permitting the seizure of historical CSLI without a warrant, intrudes on cell phone subscribers' legitimate expectations of privacy. Individuals enjoy a subjective and objectively reasonable expectation of privacy in their homes, offices, houses of worship, and other private places, even though technology enables the government to track them to and in those places without physically intruding on the private property. *Kyllo v. United States*, 533 U.S. 27, 34 (2001). CSLI provides the government with details about a person's whereabouts and movements. "Location data from a cell phone is distinguishable from traditional physical surveillance because it enables law enforcement to locate a person entirely divorced from all visual observation." *In re Application for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 849 F. Supp. 2d 526, 540 (D. Md. 2011); *see also id.* at 540-41 (describing that CSLI can be as accurate as GPS location, and that the technology can place a phone inside a specific home, even if locating a person there requires some inferences).

Even more intrusive, historical CSLI allows the government to retroactively observe a suspect via technology, as well as in the course of private and intimate personal, social, religious, and other associations, interactions, and activities. *See United States v. Jones*, 132 S. Ct. 945, 955 (2012) (citing *People v. Weaver*, 909 N.E.

2d 1195, 1199 (N.Y. 2009)) (Sotomayor, J., concurring) (electronic “monitoring generates a precise, comprehensive record of a person’s public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.”).

A cell phone user’s reasonable expectation of privacy in CSLI equals or exceeds that of GPS data. In *Jones*, the Supreme Court ruled that a warrant based on probable cause is required to support the retrieval of location data obtained by the placement of a GPS device under an individual’s automobile. While the decision was premised on a trespass theory, at least five justices recognized that an individual has a reasonable expectation of privacy with respect to long-term monitoring of his or her movements, including via a GPS device. *See Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) (“I agree with Justice Alito that, at the very least, “longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.” (citing Justice Alito’s dissent at 964)). For example, although an automobile’s movements may be public, the aggregation of the points of data established a reasonable expectation of privacy. By contrast, a cell phone may accompany its owner anywhere, including private events like a visit to a psychiatrist, a medical doctor, or a priest. Because one chooses to keep these events private, then one has a reasonable expectation of privacy in his whereabouts. The exposure of the CSLI can convert what would otherwise be a private event into a public one. Therefore, while *Jones* may protect only aggregated data, even one point of cell site location data falls within a reasonable expectation of privacy. Thus, cell

site data is more like communications data than it is like GPS information: it is private in nature rather than being public data that warrants privacy protection only when its collection creates a sufficient mosaic to expose that which would otherwise be private.¹

An individual does not surrender his reasonable expectation of privacy in CSLI by placing or receiving a call. The contention that a cell phone subscriber lacks a protectable Fourth Amendment interest in CSLI because he or she “voluntarily conveys” such information to his cell phone company is a fiction not grounded in the realities of modern cell phone usage. *See In Re Application of the United States for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d 113, 127 (E.D.N.Y. 2011) (“The fiction that the vast majority of the American population consents to warrantless government access to the records of a significant share of their movements by ‘choosing’ to carry a cell phone must be rejected.”).

Instead, such a contention relies on case law involving pen registers and business records of banks and similar entities that is inapposite to CSLI and the seizure of such electronic information under the SCA. *Smith*, discussed *supra* at page 2, is inapplicable to historical CSLI. The ruling in *Smith* is limited to phone company records of the numbers that the customer affirmatively dials from his or her phone. *Smith*, 442 U.S. at 744. The location of the cell phone customer at the time calls were made or received—unlike the numerical information affirmatively disclosed by the customer when using his phone—is information that was not

¹ This rationale was adopted by a panel on the U.S. Court of Appeals for the Eleventh Circuit in *United States v. Davis*, 754 F.3d 1205, 1216 (11th Cir. 2014). The full Eleventh Circuit subsequently granted the government’s request for review *en banc* in that case, and the panel opinion was vacated.

voluntarily conveyed by any action on his part. Nor does *Smith* purport to address records as to a subscriber's location at the time of calls. *Smith* involved landline telephones and did not address the far different context of mobile cell phone usage and cell tower location data. *See Smith*, 442 U.S. at 743 (“Regardless of his location, petitioner had to convey that number to the telephone company in precisely the same way if he wished to complete his call.”)

The Court in *Smith* found that “all subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.” 442 U.S. at 742. No such comparable information is given to cell phone users on their monthly bills with respect to their *locations* at the time of making or receiving calls.

The Court in *Smith*, relied on *United States v. Miller*, 425 U.S. 435 (1976), to support its analysis that telephone subscribers voluntarily convey to their phone company the numbers dialed on their phones. In *Miller*, the Supreme Court held that bank customers lack a reasonable expectation of privacy in information voluntarily conveyed to banks, including checks, deposit slips, and financial statements. *Miller* is wholly distinguishable from the instant case. Bank customers personally provide their banks with checks and deposit slips and receive monthly bank statements setting forth customer financial records. No cell phone customer personally provides his or her cell phone company with information concerning his whereabouts at the times calls are made or received nor does the company advise the customer of such information in its phone bill statements.

Moreover CSLI, which is not tangible or visible to cell phone user, is not a proprietary business record within a company's complete, unfettered control, such as an expense report. An individual's location and movements are not analogous to financial business data used in commercial transactions between people and entities, nor does an individual phone user affirmatively disclose to phone company employees his or her whereabouts when making and receiving calls.

Despite using an intermediary to place a phone call, cell phone customers take no affirmative steps to disclose their location to the public. CSLI is generated automatically and conveyed without any choice or overt action explicitly exposing location. The user does not knowingly and voluntarily disclose the information under his own control. Unlike dialed telephone numbers or bank deposit slips, CSLI is not subject to general understanding any more than the operation of a satellite television signal. Indeed, interpreting this cell site data requires an understanding of radio frequency engineering. *Cf. Katz v. United States*, 389 U.S. 347, 351-52 (1967) (holding that information that a person *knowingly* exposes to the *public* is not protected). Instead, it is transmitted independent of any input, control, or knowledge on the part of the cell phone user. To the extent that an unknowing, involuntary transmission of data that is automatically collected constitutes disclosure to a third party at all, a cell phone user's conduct is materially different from the active, deliberate choices made to disclose information that the Court discussed in *Smith* and *Miller*. The simple act of using, or even just carrying, a cell

phone, which has the by-product of generating location data, does not indicate a disinterest in maintaining privacy.

The involuntary conveyance of location data does not eliminate an individual's expectation of privacy, as explained by the Third Circuit. *In re Application of the U.S.*, 620 F.3d at 317-18. In that case, the court ruled that cell phone customers neither voluntarily nor knowingly share location information with their cell phone providers. *Id.* The only information shared is the number dialed, which does not indicate to the caller that placing the call will also identify the caller's location. *Id.* Further, in receiving a call, the cell phone user does not voluntarily expose anything. *Id.*

While the Fifth Circuit has reached the opposite conclusion, *see In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600, 612 (5th Cir. 2013) (agreeing with the government that cell phone users "know that they convey information about their location to their service providers when they make a call and that they voluntarily continue to make such calls"), the Fifth Circuit's findings rely on the assumption that cell phone users have a detailed understanding of how calls are transmitted. The Seventh Circuit has not yet weighed in on the issue.²

The nature of CSLI also distinguishes this case from other cases involving the so called third-party doctrine from *Miller*. As the Supreme Court has recognized, the nature of the record is critical to determining whether a person maintains a privacy

² The Seventh Circuit acknowledged the issue in *United States v. Thousand*, 558 Fed Appx. 666 (7th Cir. 2014), but expressly declined to decide the matter because it was unnecessary based on the facts of that case.

interest. *Smith*, 442 U.S. at 741. Pen registers, for example, provide the government with very limited information. *Id.* CSLI, on the other hand, is more analogous to content, in which people maintain a privacy interest, although intermediaries have access to the information, because of detail it provides the government. *In re Application*, 809 F. Supp, 2d at 124-25.

CSLI has attributes of content because of the highly personal nature of the data and the amount of information that it reveals about a person. Because cumulative CSLI, recording a person's movements over a prolonged period, "implicates sufficiently serious protected privacy concerns" it should be treated as "content, to prohibit under governmental intrusion." *Id.* at 126. "There is no meaningful distinction between content and other forms of information, the disclosure of which to the government would be equally intrusive and reveal information society values as private." *Id.* at 125 (relying on *Smith*, 442 U.S. at 741 n.5) And the content of communications is not available to the government without a warrant, even if a third party stores and has access to it.

Unlike other records that a business might generate, Congress has directed cellular service providers to protect the confidentiality of CSLI. The Wireless Communication and Public Safety Act obliges cellular service providers to protect information that they acquire solely by virtue of the fact that they provide telecommunications service to the customer. *See* 47 U.S.C. § 222 (a), (f). Although this statute does not prevent law enforcement from accessing the information, the Congressionally-mandated limit on using the information is undeniably relevant to

the legitimate expectation of privacy inquiry. In contrast, relating to the records at issue in *Miller*, Congress had specifically legislated that customers should not expect to maintain privacy in information conveyed to banks. *See Miller*, 425 U.S. at 441 (relying on 12 U.S.C. § 1829(a)(1)).

The Supreme Court has recognized that the government may not exploit evolving technologies to “erode the privacy guaranteed by the Fourth Amendment.” *Kyllo*, 533 U.S. at 34. For the government to employ technology to learn information that would be available otherwise only by means of a warrant, it must seek that warrant. *See United States v. Karo*, 468 U.S. 705, 715-16 (1984). The SCA’s lower “reasonable grounds” standard that permits the government to acquire CSLI, including for prolonged, continuous time periods, intrudes on a subjective expectation of privacy that society recognizes as reasonable and is untenable. When the Court examines the Government’s application, it should use instead the probable cause standard.

II. The government cannot meet the “reasonable grounds” standard for either type of information it seeks—let alone the probable cause standard required for the historical CSLI—and thus the government’s application should be denied.

The government requests that this Court order the seizure of 106 days of records related to Subject Phone 3. As support for the request, the government submits an affidavit from FBI Special Agent Maureen Mazzola. In her affidavit, Agent Mazzola recounts relevant portions of the investigation to date, including how the government became aware that Mr. Lang used Subject Phone 3.

Specifically, during a search of the contents of Subject Phone 1, the government observed a text message received on June 14, 2013, from Subject Phone 3 that read “Give me a call, Tyler.” (Aff. ¶14) Agent Mazzola then observed over 800 contacts between Subject Phones 1 and 3, until contact stopped on August 3, 2013. (*Id.*) While the government’s investigation may have provided evidence of contact between Mr. Lang and Mr. Johnson, it has not provided “specific and articulable facts” that there are “reasonable grounds” that the requested information is “relevant and material” to *this investigation*. 18 U.S.C. § 2703(d). By virtue of failing to meet the “reasonable grounds” standard, the government also fails to meet the higher probable cause standard for CSLI.

Agent Mazzola informs the Court that the government needs the extensive requested records from Subject Phone 3 in order to show (1) “the telephone contacts between Tyler Lang and Kevin Johnson in the months leading to the mink raid,” (2) “steps taken by Lang and Johnson in preparation for the mink raid,” and (3) “potentially the route he and Johnson took in travelling to Illinois in order to actually conduct the raid.” (Aff. ¶16)

As an initial matter, Subject Phone 3 was not located on the person of Mr. Lang or Mr. Johnson at the time of their arrest. Nor was it seized during the search of the vehicle in which Mr. Lang and Mr. Johnson were travelling. The vehicle was secured upon their arrest, until a search warrant could be obtained. Upon the execution of that search warrant, all contents of the vehicle were inventoried. Only Subject Phones 1 and 2 were recovered during the search. The government has not

provided the Court with even an inference that Subject Phone 3 was present in Illinois or that it accompanied Mr. Lang outside of California. Thus it is improbable that Subject Phone 3 contains any material information relevant to this investigation. It is also likely impossible that Subject Phone 3 contains any relevant location information, because it was not present in Illinois, or it appears, used after August 3, 2013.

The other information the government seeks is information that it already has obtained. According to Agent Mazzola, the government is aware of exactly how many contacts Subject Phones 1 and 3 had during the period in question. Moreover, the government is aware of the contents of both sides of the communications because of its examination of Subject Phone 1 (e.g. the 6/14/13 text message that reads “Give me a call, Tyler.” is a text message from Subject Phone 3, but available to be read on Subject Phone 1). The government has provided this Court with no information to suggest that new—or in the language of the statute: “material”—information will be discovered on Subject Phone 3.

To the extent that Agent Mazzola provides an alternative rationale for the government’s request in paragraph 17 of the affidavit, it fairs no better. (Aff. ¶17 “The FBI further plans to use the information requested in the attached Application to identify and locate individuals who are in contact with the offender or offenders and may be able to provide information relevant to the investigation.”) The government fails to explain how historical CSLI will help them locate individuals who may be able to provide relevant information. Although toll records may provide

other telephone numbers to the government, this would be nothing more than a fishing expedition. The government's attempt to meet the reasonable grounds standard focused entirely on the relationship between Mr. Lang and Mr. Johnson. The government provided no information to connect any other individuals to the charged offense, or even to Subject Phone 3.

As discussed above, the government has failed to provide this Court with all the requirements of the SCA. It has provided no specific and articulable facts showing that there are reasonable grounds that either the historical CSLI or historical toll record information for Subject Phone 3 will provide relevant and material information to this ongoing criminal investigation. Because the government has not met the lower "reasonable grounds" standard, for the same reasons it has not met the higher "probable cause" standard required for the issuance of a warrant for historical CSLI.

For these reasons, Mr. Lang respectfully requests that this Court deny the government's application for an order under 18 U.S.C. 2703(d) directing Verizon to provide historical CSLI information and toll records from the period of May 1, 2013 through August 14, 2013.

Respectfully submitted,

FEDERAL DEFENDER PROGRAM
Carol A. Brook,
Executive Director

By: s/ Geoffrey M. Meyer
Geoffrey M. Meyer
Attorney for Tyler Lang

FEDERAL DEFENDER PROGRAM
55 E. Monroe Street, Suite 2800
Chicago, Illinois 60603
(312) 621-8326

CERTIFICATE OF SERVICE

The undersigned, **Geoffrey M. Meyer**, an attorney with the Federal Defender Program, hereby certifies that in accordance with Fed. R. Crim. P. 49, Fed. R. Civ. P. 5, LR 5.5, and the General Order on Electronic Case Filing (ECF), the following document:

DEFENDANT TYLER LANG'S RESPONSE TO THE
GOVERNMENT'S APPLICATION FOR AN ORDER RELATING TO SUBJECT PHONE 3

was served pursuant to the district court's ECF system as to ECF filers, if any, and was sent by first-class mail/hand delivery on **December 2, 2014**, to counsel/parties that are non-ECF filers.

By: s/ Geoffrey M. Meyer
Geoffrey M. Meyer
FEDERAL DEFENDER PROGRAM
55 E. Monroe Street, Suite 2800
Chicago, Illinois 60603
(312) 621-8326